Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Protecting Against National Security	)	WC Docket No. 18-89
Threats to the Communications Supply	)	
Chain Through FCC Programs	)	

COMMENTS OF NETNUMBER, INC.

Steven A. Augustino
Edward A. Yorkgitis, Jr.
J. Bradford Currier
Kelley Drye & Warren LLP
3050 K Street, NW, Suite 400
Washington, D.C. 20007
(202) 342-8400

Counsel to NetNumber, Inc.

May 20, 2020

TABLE OF CONTENTS

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Protecting Against National Security	)	WC Docket No. 18-89
Threats to the Communications Supply	)	
Chain Through FCC Programs	)	

COMMENTS OF NETNUMBER, INC.

NetNumber, Inc. ("NetNumber"), by its attorneys, hereby responds to the *Public Notice* issued by the Commission on the applicability of Section 4 of the Secure and Trusted Communications Networks Act of 2019 ("Section 4") to its rulemaking on protecting against national security threats to the communications supply chain.[1]

I. INTRODUCTION AND SUMMARY

Founded in 1999, NetNumber is a leading provider of core network signaling, routing, security, and database solutions to mobile, fixed, and intermediate service providers. NetNumber is U.S.-owned, U.S.-based, and its equipment is U.S.-manufactured. Through its innovative TITAN platform, the company offers subscriber data management solutions, such as global number portability, toll-free routing, calling-name lookup, and least-cost routing. Used by more than 250 service providers, TITAN is the industry's most robust Centralized Signaling and Routing Control platform, providing a common infrastructure for all signaling control, routing, security, and subscriber database solutions in a network. NetNumber offers customers several

[1] *Wireline Competition Bureau Seeks Comment on the Applicability of Section 4 of the Secure and Trusted Commc'ns Networks Act of 2019 to the Commission's Rulemaking on Protecting Against Nat'l Sec. Threats to the Commc'ns Supply Chain*, WC Docket No. 18-89, Public Notice, DA 20-406 (Apr. 13, 2020) ("*Public Notice*"). *See* Pub L. 116-124, 133 Stat. 158, § 4 (2020) (codified at 47 U.S.C. § 1603) ("Section 4"); *Protecting Against Nat'l Sec. Threats to the Commc'ns Supply Chain Through FCC Programs, et al.*, WC Docket No. 18-89, *et al.*, Report and Order, Further Notice of Proposed Rulemaking, and Order, 34 FCC Rcd 11423 (2019) ("*Supply Chain FNPRM*").

deployment options for its products, including onsite deployments through servers and other hardware as well as virtual deployments through NetNumber software applications and Cloud Service Centers.

NetNumber welcomes the opportunity to bring its more than 20 years of experience in providing network solutions to bear and offer insight on Section 4's impact on the Commission's notable efforts to protect the communications supply chain.[2] NetNumber agrees with the Commission that "[e]nsuring the safety, reliability, and security of the nation's communications networks is vital not only to fulfilling the purpose of the [Communications] Act but to furthering the public interest."[3] The company also shares the Commission's concern with the national security risks posed by use of the equipment and services offered by Huawei Technologies Company ("Huawei") and ZTE Corporation ("ZTE").[4] NetNumber provides its customers with secure network solutions comparable (or often superior) to these companies' products. Section 4's touchstone is reducing the risks "covered" companies present to U.S. communications networks and the underlying supply chain.[5] To further this objective, Section 4 directs the Commission to establish a reimbursement program for qualifying "providers of advanced communications service" to remove, replace, and dispose of covered equipment and services in

---

2 NetNumber has won multiple awards for its network security solutions and works with its industry association partners in the CCA, CTIA, GSMA, and other organizations to help ensure the security of communications services and equipment.

3 *Supply Chain FNPRM* at para. 124.

4 *Id. See id.* at paras. 43-63 (provisionally designating Huawei and ZTE as "covered" companies posing a threat to national security).

5 *Chairman Pai Statement on Enactment of the Secure and Trusted Commc'ns Networks Act*, FCC Statement (Mar. 12, 2020), available at https://docs.fcc.gov/public/attachments/DOC-363006A1.pdf (stating the law will help service providers "end their reliance on manufacturers that pose national security threats" and facilitate the transition "to infrastructure provided by more trusted vendors").

their networks (the "Reimbursement Program").[6] NetNumber submits that the Reimbursement Program should provide an orderly, practical, and equitable transition away from covered equipment and services offered by companies identified as posing national security risks (*e.g.*, Huawei and ZTE) to network solutions provided by more-trusted and qualified vendors ("trusted vendors").[7] Specifically, NetNumber recommends that the Commission develop a competitively-neutral list of suggested replacement solutions, include virtual equipment and services on such list, interpret the scope of advanced communications services broadly – for example, to cover deployment and project costs, and ensure equitable reimbursement distribution through tailored funding caps and flexible replacement timeframes to account for practical realities and challenges.

II. THE COMMISSION SHOULD DEVELOP A COMPETITIVELY-NEUTRAL LIST OF SUGGESTED REPLACEMENT SOLUTIONS

In the *Public Notice*, the Commission inquires about the best way to develop a list of suggested replacement equipment and services, as required by Section 4.[8] Section 4 states that the list may not favor certain solutions among those that can serve as adequate replacements for covered equipment and services.[9] NetNumber concurs with the Commission that clearly defining available replacement solutions will reduce the burden imposed on service providers

---

6 47 U.S.C. § 1603(a).

7 The Commission could establish criteria for designating trusted vendors using a "totality-of-the-circumstances approach" that would consider, among other factors, whether a vendor is publicly traded, in good standing with the Committee on Foreign Investment in the United States (or its successor), a Customs-Trade Partnership against Terrorism verified provider, and has a history of complying with U.S. laws and regulations. *See* Letter from Brian Hendricks, Head of Policy and Government Relations, Americas Region, Nokia, to Marlene H. Dortch, Secretary, Federal Communications Commission, WC Docket No. 18-89, 2-3 (April 9, 2018).

8 *Public Notice* at 3-4 (citing 47 U.S.C. § 1603(d)(1)(A)).

9 *Id.* (citing 47 U.S.C. § 1603(d)(1)(B)).

that must remove covered equipment or services from their networks.[10] NetNumber submits that the Commission should develop the suggested replacement list in a competitively-neutral manner, creating a helpful information source for impacted service providers without endorsing any vendor over another capable of providing suitable replacement equipment or services in a timely manner.

Through its work with existing and prospective customers, NetNumber has gained substantial knowledge of the core network functions currently performed by Huawei/ZTE equipment and services. The attached chart identifies those functions that NetNumber understands Huawei/ZTE equipment or services may be performing.[11] This chart and similar information received from other stakeholders in this proceeding can serve as a "jumping-off" point for the Commission's development of the list. However, as a second-stage development effort, NetNumber recommends that the Commission launch a more targeted data collection to ensure the list will be as comprehensive as possible.[12] In particular, NetNumber recommends a Public Notice soliciting information from network solutions providers (including core network, radio access network, evolved packet core network, and 5G network vendors) on the communications equipment and services they provide. The Public Notice should ask providers to pair their current network solutions (as documented in public sources)[13] with the core network

---

10 *Supply Chain FNPRM* at para. 136.

11 *See* Attachment.

12 The Commission often requests industry input on the types of services that should be supported by its funding programs. *See, e.g.*, 47 C.F.R. § 54.502(e) (requiring the Commission to seek comment on the proposed eligible services list for the E-Rate program each year).

13 Such sources could include vendor websites and responses to public requests for proposal as well as supply lists, product documentation, and information found in public webinars.

functions presently supported by Huawei and ZTE that their solutions could replace.[14] The Commission should then develop and have its preliminary list reviewed by a qualified, unaffiliated engineer under contract with the Commission or submitted for further input by key industry associations – looking to both American and European organizations to get the broadest viewpoints (*e.g.*, 3GPP, GSMA, and ETSI).

To ensure the suggested replacement list is comprehensive, NetNumber urges the Commission to include *all* equipment and services provided by trusted vendors for each core network function. As recognized in the *Public Notice*, this approach will ease the Commission's administrative burden by eliminating the need to specifically list each model/version of replacement equipment or service that trusted vendors provide.[15] The Commission should accept information from trusted vendors to update the list on a periodic basis, as trusted vendors make available for deployment additional solutions for additional core network functions.[16] NetNumber recommends that trusted vendors should be required to notify the Commission on a semiannual basis if they no longer provide solutions for listed core network functions.

By encouraging comprehensiveness and regular updates, the Commission's suggested replacement list will provide valuable information to impacted service providers without

---

14 Alternatively, the Commission could identify selected vendors in advance and initiate a closed solicitation process to develop the list. Such selection could follow a deep-dive workshop held by the Commission with U.S. vendors that demonstrate they meet basic qualifications as either a core network, radio access network, evolved packet core network, or 5G network vendor through submission of a prequalification form or other screening mechanism.

15 *See Public Notice* at 4 (seeking comment of whether the list should "simply include all equipment and services from certain companies").

16 In the alternative, the Commission could update the list on a quarterly or semiannual basis. The Commission should provide reimbursement for products from listed vendors "that are safer or more secure than the replaced equipment or services" to ensure service providers remain current with industry standards. *See Supply Chain FNPRM* at para. 140.

endorsing any particular vendor or solution. Another benefit of this approach is that it gives service providers, whether impacted by the Replacement Program or not, information on new and upgraded network solutions developed by trusted vendors as they become available.

III. THE COMMISSION SHOULD INCLUDE SUPPLIERS OF VIRTUAL SOLUTIONS ON ITS SUGGESTED REPLACEMENT LIST

The Commission asks in the *Public Notice* whether providers of virtual communications equipment and services should be included on its suggested replacement list.[17] The answer is yes. Section 4 dictates that the list include "suggested replacements of *both* physical and virtual communications equipment . . . and services."[18] In addition, the Commission highlighted the risks of unsecure "virtualized" network infrastructure when designating Huawei and ZTE as covered companies.[19] The Commission can help service providers combat these risks by including suppliers of virtual equipment and services on its suggested replacement list.

Including virtual solutions on the list comports with market realities. In today's communications networks, a variety of architectures support core network functions. While some vendors build products designed to work on specific-purpose hardware solutions, other vendors build software that can be deployed on both commercial off-the-shelf hardware solutions or in virtual environments. A range of vendors build hardware used to create the virtual environments for which software vendors can install their products (*e.g.*, Cisco, HP, and others). Software vendor products also can reside "in the cloud," where solutions are centralized and accessible from a range of sources and networks. In addition to hardware-based deployments, NetNumber's solutions can be deployed onto most virtual network infrastructure. Indeed,

---

17 *Public Notice* at 4.

18 47 U.S.C. § 1603(d)(1)(A) (emphasis added).

19 *Supply Chain FNPRM* at para. 68.

NetNumber has found that making carrier infrastructure virtual solution-ready can simplify and accelerate the network equipment and service replacement process.[20]

Because impacted service providers can utilize both hardware and software solutions to replace the functionality provided by covered equipment and services, NetNumber urges the Commission to list trusted vendors whose products can be deployed into virtual and cloud environments, in addition to providers of hardware-specific solutions.

IV. THE COMMISSION SHOULD INTERPRET "ADVANCED COMMUNICATIONS SERVICES" BROADLY

The Section 4 Reimbursement Program only is available to providers of advanced communications service ("ACS") that must replace covered equipment or services in their networks.[21] For Section 4, ACS has the same meaning as the term "advanced telecommunications capability" found in Section 706 of the Telecommunications Act of 1996.[22] Section 706 defines advanced telecommunications capability as "high-speed, switched, broadband telecommunications capability that enables users to originate and receive high-quality voice, data, graphics, and video telecommunications using any technology."[23] While this definition potentially covers many network solutions, the Commission should interpret ACS in a way that covers all equipment and services that could pose a national security risk now or in the future.

A broad ACS interpretation is appropriate given the significant number of applications in which Huawei/ZTE equipment and services are used today. Common examples of networks

---

20 Thus, NetNumber submits that, if the service provider deploys "carrier-grade" infrastructure, then it makes sense for the Commission to encourage the move to more virtualized networks.

21 47 U.S.C. § 1603(a).

22 *See* 47 U.S.C. § 1608(1).

23 47 U.S.C. § 1302(d).

where Huawei/ZTE equipment and services are deployed in the United States include those used for: (1) wireless communications (as well as associated signaling); (2) wireline communications (as well as associated signaling); (3) cable telephony; (4) messaging; (5) private networks for enterprise, utility, or government entities; and (6) mobile virtual network operators. In addition, NetNumber solutions often serve as a robust replacement for Huawei/ZTE equipment and services used by interconnected and non-interconnected VoIP providers, intermediate providers acting as go-betweens interconnecting other networks, electronic messaging providers, and interoperable video conferencing providers. Thus, NetNumber submits that the Commission should interpret ACS broadly to include, at a minimum, the offerings of fixed and mobile broadband providers as well as interconnected and non-interconnected VoIP, electronic messaging, and interoperable video conferencing providers.[24] The ACS interpretation should include the services of providers serving end users, but also those that function on an intermediate basis and provide capability and connectivity within the network to make retail ACS possible. The Commission also should consider exercising its ancillary authority to include other services in the ACS definition, including those that may be provided by entities that offer "telecommunications" but not telecommunications services, such as providers of large enterprise/government private networks as well as providers of cable telephony services (who often offer VoIP products).[25] In interpreting ACS broadly under the Reimbursement Program,

---

[24] *See Inquiry Concerning Deployments of Advanced Telecomms. Capability to All Americans in a Reasonable and Timely Fashion*, GN Docket No. 18-238, 2019 Broadband Deployment Report, 34 FCC Rcd 3857 (2019) (defining advanced telecommunications capability for broadband); *see also* 47 U.S.C. § 153(1) (defining ACS as including interconnected and non-interconnected VoIP, electronic messaging, and interoperable video conferencing under the Twenty-First Century Communications and Video Accessibility Act of 2010).

[25] *See, e.g.*, 47 U.S.C. §§ 151, 154(i).

the Commission will allow a wide range of service providers to receive the support necessary to remove covered equipment and services, thereby securing their networks.

V. THE COMMISSION SHOULD ENSURE EQUITABLE REIMBURSEMENT DISTRIBUTION THROUGH TAILORED FUNDING CAPS AND FLEXIBLE TIMELINES

The Commission seeks comment in the *Public Notice* on how it can ensure an equitable distribution of reimbursement funding across applicants, as required by Section 4.[26] NetNumber submits that the Reimbursement Program should include funding caps to advance the objective of replacing covered equipment and services nationwide without favoring any particular region or customer segment. However, such caps must be tailored to provide fair compensation for the full deployment cost for replacement equipment and services within a provider's network.

First, the Commission should tie reimbursement caps to the size of network deployments. For example, a large multistate or international interconnection carrier may have spent considerably more on covered equipment and services requiring replacement than a rural wireless carrier. Second, the Commission should consider reimbursement caps that vary depending on service provider type. For example, the replacement costs for covered equipment and services in a 5G network may be significantly more than the replacement costs associated with a 3G network or other legacy service due to the service provider's network complexity. The Commission therefore should cap reimbursement for service providers at their estimated replacement costs for covered equipment and services in their networks.[27] In doing so, the Commission should consider issuing a cost catalog with preapproved reimbursement amounts,

---

26 *Public Notice* at 2 (citing 47 U.S.C. § 1603(d)(5)).

27 *See* 47 U.S.C. § 1603(d)(2) (establishing service provider cost estimate submission process).

allowing service providers to better scale replacements based on network size and account for network design in their replacement projects.

Flexible replacement timelines also would facilitate equitable treatment of service providers under the Reimbursement Program. Section 4 requires reimbursement recipients to complete the replacement of covered equipment and services within one year of receiving funding, with extensions available under certain circumstances.[28] In NetNumber's experience working with more than 250 carriers globally, most service providers only can absorb a certain number of projects in a given year due to the precariousness of network upgrades and the limited amount of skilled personnel available to work on such upgrades. Core network infrastructure projects typically run from 6 to 8 months to as long as 12 to 18 months. Consequently, a one-year replacement deadline may be infeasible for many service providers that must replace covered equipment or services without extensions or other special accommodations.

In light of the variation among service providers in the amount of covered equipment and services in their networks, NetNumber submits that the Reimbursement Program should allow for phased milestones and corresponding reimbursements to better manage larger-scale replacement projects while adhering to Section 4's timeline requirements.[29] Phased replacement milestones are appropriate, including varying timelines for new equipment and service deployment as well as network testing.[30] Thus, NetNumber recommends that the Commission establish a set of phased replacement milestones to provide elasticity for service providers with

---

28 47 U.S.C. § 1603(d)(6).

29 *See Supply Chain FNPRM* at para. 155 (seeking comment on whether a phased replacement approach is appropriate due to the varying size and complexity of service provider networks).

30 In particular, NetNumber has found that replacement of in-depth data and routing systems as well as subsequent network testing can be particularly time-consuming, especially when a large amount of subscriber data needs to be migrated to a replacement solution.

networks varying in size and complexity. The Commission also should encourage efficiencies by allowing service providers to synchronize Section 4 replacement efforts with other pending network projects and take account of seasonality issues.[31] In sum, the Commission should adopt flexible timeframes for the replacement of covered equipment and services to avoid imposing impractical deadlines on service providers in securing their networks.

VI. CONCLUSION

The Section 4 Reimbursement Program is critical to ensuring the future security of U.S. communications networks. With the improvements recommended by NetNumber above, the Commission will arm service providers with the support necessary to secure their networks and the underlying supply chain.

Respectfully Submitted,

Steven A. Augustino
Edward A. Yorkgitis, Jr.
J. Bradford Currier
Kelley Drye & Warren LLP
3050 K Street, NW, Suite 400
Washington, D.C. 20007
(202) 342-8400

Counsel to NetNumber, Inc.

May 20, 2020

[31] For example, carriers typically undertake far less network upgrade work during holiday seasons and the summer. As a result, most such work takes place in the first half of each year.

ATTACHMENT

Huawei and ZTE Rip and Replace items

	CORE NETWORK APPLICATIONS		
Subscriber Data Management	HSS	Home Subscriber Services	
	HLR	Home Location Services	
	AuC	Authentication Control	
	EIR	Equipement Identity Register	
Signalling & Routing	STP	Signalling Transfer Point	
	DSC	Diameter Signalling Controller	
	NP	Number Portability	
	IWF	Interworking Function	
	SRM	SIP Routing Manager	
	ENUM	ENUM	
Security	SigFW	Signalling Security Firewall	
3G, 4G Mobile Core	MPC (3G)	SGSN	Serving GPRS Support Node
		GGSN	Gateway GPRS Support Node
		PDG	Packet Data Gateway
	EPC (4G)	MME	Mobility Management Entity
		SGW	Serving Gateway
		PGW	Packet Data Network Gateway
5G Core Network	Signalling & Routing	SCP	Signalling Control Platform
		NRF	NF Repository Function
		BSF	Binding Support Function
		NSSF	Network Slice Selection Function
		UDSF	Unstructured Data Storage Function
	Subscriber Data Mngmt	UDM	Unified Data Management
		ARFP/SIDF	Authentication Credential Repository
		AUSF	Authentication Server Function
		UDR	Unified Data Repository
	Security	SEPP	Security Edge Protection Proxy
		EIR	5G Equipment Identity Register

Cloud Hosted Data Services	
Global Data Services	
	Number Portability Data (90+ countries)
	Toll-Free Data
	Spam/Fraud Data
	Portability History data
	CNAM data

Notes:

Applications can be deployed directly in premise or used in a private/public cloud deployment